**Middle East Technical University**

**Department:** Computer Science and Engineering

**Year:** Fall 2024-2025

**Course:** Discrete Computational Structures

**Student's Solution**

**Name Surname:** <Abdullah Burkan Bereketoğlu> **Student ID:** <2355170>

# 1 Question 1

1. For our proof let's first look at base case then from that follow induction step.

   **Base Case ($n = 1$):** on the left-hand side (LHS) we have:

$$\sum_{j=1}^{1} j(j+1)\cdots(j+k-1) = 1 \cdot 2 \cdot 3 \cdots k = k!.$$

   The right-hand side (RHS) is then:

$$\frac{1 \cdot 2 \cdot 3 \cdots (k+1)}{k+1} = \frac{(k+1)!}{k+1} = k!.$$

   Which shows equivalence, hence formulation holds for base case.

   **Inductive Step:** So, now assume that it also holds for $n \geq 1$, i.e.,

$$\sum_{j=1}^{n} j(j+1)\cdots(j+k-1) = \frac{n(n+1)(n+2)\cdots(n+k)}{k+1}.$$

   We must show it holds for $n+1$ as in mathematical induction. So we would be looking at:

$$\sum_{j=1}^{n+1} j(j+1)\cdots(j+k-1) = \left(\sum_{j=1}^{n} j(j+1)\cdots(j+k-1)\right) + (n+1)(n+2)\cdots(n+k).$$

   Using the inductive hypothesis, RHS equals to for $n+1$):

$$= \frac{n(n+1)(n+2)\cdots(n+k)}{k+1} + (n+1)(n+2)\cdots(n+k).$$

   this shows $n+1$ and $n$ together then factor out the $(n+1)(n+2)\cdots(n+k)$ and get;

$$= (n+1)(n+2)\cdots(n+k)\left[\frac{n}{k+1} + 1\right].$$

Inside the bracket can be simplified as;

$$\frac{n}{k+1}+1=\frac{n+(k+1)}{k+1}=\frac{n+k+1}{k+1}.$$

Henceforth;

$$\sum_{j=1}^{n+1} j(j+1)\cdots(j+k-1)=(n+1)(n+2)\cdots(n+k)\cdot\frac{n+k+1}{k+1}.$$

We can see that $(n+1)(n+2)\cdots(n+k)(n+k+1)$ is directly $n+1$ of LHS and RHS. Hence:

$$\sum_{j=1}^{n+1} j(j+1)\cdots(j+k-1)=\frac{(n+1)(n+2)\cdots(n+k+1)}{k+1}.$$

By mathematical induction we can state that, the formula holds for all $n \in \mathbb{N}_0$.

2. 1. Since $p$ is a prime, Fermat's Little Theorem state the following:

$$x^{p-1} \equiv 1 \pmod{p},$$

for any integer $x$ such that $\gcd(x,p)=1$, meaning x is not divisible by p.

2. By assumption $y$ is stated as the smallest positive integer such that:

$$x^{y} \equiv 1 \pmod{p}.$$

Which means $y$ is the smallest power of x with remainder 1 with division to p.

3. From Fermat's Little Theorem, we can deduce that $x^{p-1} \equiv 1 \pmod{p}$. Leading to the implication of $y \mid (p-1)$.

Hence, let $p-1=ay+r$, where $a$ is quotient and $b$ is remainder when it $p-1$ divided by $y$, with b value being $0 \leq b < y$. Thus;

$$x^{p-1}=x^{ay+b}=(x^{y})^{a}\cdot x^{b} \equiv 1^{a}\cdot x^{b} \equiv x^{b} \pmod{p}.$$

We do know from Fermat's Little Theorem $x^{p-1} \equiv 1 \pmod{p}$ also $x^{y} \equiv 1 \pmod{p}$, which indicates following $x^{b} \equiv 1 \pmod{p}$. So for minimum $y$ we use $b=0$. Hence we end up with, $y \mid (p-1)$.

3. Problem expects subset proof for binomial expansion or whole combination options. For that consider the expansion of $(1+1)^{n}$ for a simple start, leading to;

$$(1+1)^{n}=\sum_{k=0}^{n}\binom{n}{k}1^{n-k}\cdot 1^{k}=\sum_{k=0}^{n}\binom{n}{k}.$$

Since $(1+1)^n = 2^n$, we can directly say the result as:

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n.$$

We can also prove with induction as it is stated in the hint of the question. Again consider base case $n = 0$,

$$\sum_{k=0}^{0} \binom{0}{k} = \binom{0}{0} = 1 = 2^0.$$

Then at inductive step of $n$,

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n.$$

for inductive step $n+1$ must hold and this indicates, holds for every value. With Pascal's identity:

$$\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1},$$

we get;

$$\sum_{k=0}^{n+1} \binom{n+1}{k} = \binom{n+1}{0} + \sum_{k=1}^{n} \left( \binom{n}{k} + \binom{n}{k-1} \right) + \binom{n+1}{n+1}.$$

which gives as a result.

$$\sum_{k=0}^{n+1} \binom{n+1}{k} = 2^{n+1}.$$

So with mathematical induction we can state that by inductive step shows the proof we get,

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n.$$

and it holds for all, $n \in \mathbb{N}$.

# 2 Question 2

**2.1:** For the proof let $n > 1$ and it to be an integer. We show by induction that $n$ can be written as a product of primes, being either the prime or a product of values that can be represented as the prime. Although it is not graded.

**For Base Case:** $n = 2$, $n$ is a prime number, and hence the statement is true since $n$ is a product of itself.

**For Inductive Step:** Assume that the statement holds for all integers that are in the range $2 \leq k \leq m$, and every integer $k$ can be defined as a product of primes. So consider $m + 1$.

- If $m + 1$ is prime, then it leads to being a product of itself, which is directly proved.
- On the other hand, if $m+1$ is not prime, then $m+1 = a \cdot b$, where $a, b < m+1$. By induction, it leads to $a$ and $b$ can be defined as a product of primes. Hence, $m + 1$ is written as $a$ and $b$, it is also written as product of primes.

Therefore, by induction, every integer bigger than 1 can be shown as product of such primes.

**2.2:**

It is similar to the proof made in part one, so following part one.

We will get to prove these two subjects:

1. Existence shows that, we can write each as $n > 1$ product of primes.
2. Uniqueness represents the unique order of factors up to these factors.

The existence part is already proven at 2.1. Hence, prove uniqueness to prove the state.

Assume $n > 1$ has two prime factorizations $p$ and $q$:

$$n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_m,$$

where $p_1, p_2, \ldots, p_k$ and $q_1, q_2, \ldots, q_m$ are primes. Since $p_1 \mid q_1 q_2 \cdots q_m$, and we have two prime factorizations, $p_1$ is able to divide at least one of $q_i$. Let's assume $p_1 = q_1$ for simplicity of ordering. Then cancel out $p_1 = q_1$ from both sides and get:

$$p_2 p_3 \cdots p_k = q_2 q_3 \cdots q_m.$$

For repeating this step inductively we will deduce both factorizations up to the order must be identical.

Leading that prime factorization for $n$ is unique.

**2.3:**

Power sums $p_k$, and the elementary symmetric polynomials $e_i$ are related with Newton-Girard formulas or Newton's identities, they can be shown as;

$$k \cdot e_k = \sum_{i=1}^{k} (-1)^{i-1} e_{k-i} p_i, \quad \text{for } 1 \leq k \leq n,$$

and for $k > n$:

$$0 = \sum_{i=k-n}^{k} (-1)^{i-1} e_{k-i} p_i.$$

**1. Base Case k = 1:** First elementary symmetric polynomial can be given as:

$$e_1 = x_1 + x_2 + \cdots + x_n.$$

First power sum is;

$$p_1 = x_1 + x_2 + \cdots + x_n.$$

it shows that

$$1 \cdot e_1 = p_1.$$

**2. General Case is ($k \geq 2$):** With the polynomial of roots $x_1, x_2, \ldots, x_n$:

$$P(t) = (t - x_1)(t - x_2) \cdots (t - x_n).$$

by expansion of $P(t)$, we get:

$$P(t) = t^n - e_1 t^{n-1} + e_2 t^{n-2} - \cdots + (-1)^n e_n.$$

For the roots of $P(t)$ as$x_i$ , we have $P(x_i) = 0$. Then substitute it to function as $t = x_i$ and get:

$$x_i^n = e_1 x_i^{n-1} - e_2 x_i^{n-2} + \cdots + (-1)^n e_n.$$

Multiply sides with $x_i^{k-n}$ (for $k \geq n$) and sum over all $i$:

$$\sum_{i=1}^{n} x_i^k = e_1 \sum_{i=1}^{n} x_i^{k-1} - e_2 \sum_{i=1}^{n} x_i^{k-2} + \cdots + (-1)^n e_n \sum_{i=1}^{n} x_i^{k-n}.$$

LHS indicates the power sum and RHS shows the prior power sums and elementary symmetric polynomials.

**3. Inductive Step** So for assuming the formula holds for all $j < k$, with the recursive relation at general case, we can verify the identity for $k$, leading to Newton's identities hold for all $k$.

**2.4**

**1. Symmetry Definition:** If a polynomial does not change under any permutation of it's variables, we say it is symmetricA polynomial $f(x_1, x_2, \ldots, x_n)$ is symmetric. This means that;

$$f(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) = f(x_1, \ldots, x_n),$$

for any such permutation $\sigma$ of $\{1, \ldots, n\}$.

**2. Elementary Symmetric Polynomials:** The elementary symmetric polynomials are defined as;

$$e_k(x_1, \ldots, x_n) = \sum_{1 \leq i_1 < i_2 < \cdots < i_k \leq n} x_{i_1} x_{i_2} \cdots x_{i_k}.$$

by its definition they are elementary and symmetric.

**3. Symmetric Polynomials based on Elementary Symmetric Polynomials**: Any symmetric monomial (a polynomial with one term) and they can be shown as polynomial in elementary symmetric polynomials. Hence, we see that symmetric sums of monomials need to involve only fundamental symmetric polynomials.

Such as a symmetrical monomial polynomial is as;

$$x_1^2 + x_2^2 + \cdots + x_n^2$$

can be written as; $e_1$ and$e_2$.

**4. Existence of $F \in R[y_1, \ldots, y_n]$**: There exist an $F$ such that:

$$f(x_1, \ldots, x_n) = F(e_1, \ldots, e_n).$$

for the symmetric polynomial structure and the symmetric polynomial ring.

These four steps lead to the fact that any symmetric polynomial $f$ can be expressed as elementary symmetric polynomials.

# 3 Question 3

A multiset $(S, f)$ defined as a set with repetitions allowed, where $S$ is a set and $f : S \to \mathbb{N}_0$. Where it is defined as $\{a_1^{f(a_1)}, \dots, a_n^{f(a_n)}\}$. Such as, $\{1, 1, 2, 3, 4, 4\}$ is a 4-multiset (of size 6) with the set $\{1, 2, 3, 4\}$ and can be denoted as $\{1^2, 2^1, 3^1, 4^2\}$.

1. Since, by definition multiset allows repetition and here we are finding count of the distribution ways of $n$ identical onjects to $c$ distinct bins.

   Similar to * and — rule (star and bar theorem of filling), we define the theorem as

   - Letting $n$ stars as the objects we distribute to bins.
   - To divide to $c$ bins, we require $c - 1$ bars, hence dividers.
   - Hence total number of symbols (bars and stars or dividers and elements) $n + (c - 1)$: $n$ elements and $c - 1$ dividers.
   - For to determine distribution of such system we select either $n$ positions or similarly and equivalently $c - 1$ positions for the dividers out of $n + c - 1$ total positions(total set).

   Hence, we get the total number of arrangements as;

   $$M(c, n) = \binom{c + n - 1}{n}.$$

2. We can describe the problem as distribution $13^2 = 169$ identical objects to 13-1 distinct bins, where we define each bin with $x_i$ (with $x_i \geq 0$).

   By 3.1, we get the number of solutions from,

   $$M(c, n) = \binom{c + n - 1}{n}.$$

   leading to,

   $$M(12, 169) = \binom{12 + 169 - 1}{169}.$$

   By the symmetry in binomial coefficients:

   $$\binom{180}{169} = \binom{180}{11}.$$

   Hence solution can be given as such as the latter one.

3. As first digit cannot be 0, which means $d_1 \neq 0$, so let the seven-digit positive integer be $d_1d_2d_3d_4d_5d_6d_7$, for $d_i \in \{0, 1, 2, \dots, 9\}$ and $2 \leq i \leq 7$, for to be a seven-digit number.

To be able to find numbers divisible by 3, we need $d_1 + d_2 + d_3 + d_4 + d_5 + d_6 + d_7$ divisible by 3. By total possibility with first only with 9 options we have $9 * 10^6$ total seven-digit numbers. For total 3 divisible one's we get;

$$\text{Total divisible by } 3 = 10^6 * 3.$$

With inclusion-exclusion, we know total as above, yet if no digit is 9 then we will have

$$9^6 * 3.$$

So, since we want one's with 9 remove this one and get;

$$3 \cdot 10^6 - 3 \cdot 9^6$$

as the final result

# 4 Question 4

Since the question already defines what is a regular $n$-gon we can directly continue with sub-questions

1. A symmetry of a Regular $n$-gon can be said consisting of whole rigid transformations mapping onto itself. These preserve distance and angles and can be defined as:

   - $n$ rotations, with inclusion of identity rotation $r^0$, also $r^1$ with a definition a rotation as$\frac{2\pi}{n}$ radians, and up to $r^{n-1}$.
   - $n$ reflections on symmetry axes, for each axis passing through a vertex or center and midpoint.

   This leads to n + n = 2n as cardinality, so total number of symmetries as follows:

   $$|D_n| = 2n.$$

   This corresponds$D_n$ to be finite with a cardinality of $2n$.

2. With the rules given in the question as Closure, Order of Rotation, Order of Reflection and Conjugation Relation.

   We can prove the isomorphism of set S by r and s under function composition with the rules.

   The set $S$ that is with rotation $r$ and reflection $s$ satisfies dihedral group properties $D_n$. The verification can be defined as:

   (a) **Closure:** Two rotations lead to another rotation and a rotation and reflection is a reflection. Meaning, $S$ is closed under composition

   (b) **Order of Rotation:** Full rotation is identity transformation with full being $2\pi$ and $r^n = e$. Meaning that rotations form a cyclic group of order $n$.

   (c) **Order of Reflection:** Twice reflection on same axis get us back to the original orientation, leading reflections have order 2 with $s^2 = e$.

   (d) **Conjugation Relation:** Reflection given as $s$ conjugates with rotation$r$ as:

   $$s \circ r \circ s^{-1} = r^{-1}.$$

   This happens due to reflections lead to reverse orientation with inverting the direction of rotation

   We deduced that $S$ satisfying all the properties we can say it is isomorphic to the dihedral group $D_n$, which defines symmetries of a regular $n$-gon.

3. With equivalence relation on$D_n$ for $a, b \in D_n$ and $a \sim b$ iff there is such an instance of $t \in D_n$ as;

   $$b = t \circ a \circ t^{-1}.$$

   By the above equation elements are grouped into conjugacy classes. From that we get:

- Such rotations only conjugate to other rotations.
- Such reflections as s are also similar by only conjugate to other reflections.

Hence, the conjugacy classes of $D_n$ are:

- Exist single class for identity $e$.
- $\frac{n}{2}$ rotation classes, due rotations of $k$ and $n-k \pmod n$ are conjugate to each other.
- $n$ reflection classes, due to each reflection only conjugates to itself.

Hence, with e = 1 and $\frac{n}{2}$ rotation and n reflection we have ;

$$1+\frac{n}{2}+n.$$

as total conjugacy class count.